AMENDMENTS TO CLAIMS

Claim 1 (currently amended): A timecode generation method comprising:

receiving an encryption key and an implemented encryption method;

for each one of a plurality of frames, receiving a timecode and an associated presentation time stamp (PTS) associated with the one frame;

for each one of the plurality of frames, encrypting the timecode associated with the one frame using the encryption key and the implemented encryption method, thereby producing a plurality of encrypted timecodes; ~~and~~

for each one of the plurality of encrypted timecodes, placing the encrypted timecode in an encryption container, thereby producing a plurality of encryption containers, each containing an encrypted timecode; and

~~at a time associated with the associated PTS associated with the one frame,~~ for each one of the plurality of frames, for a time associated with the associated PTS associated with the one frame, inserting the encryption container containing the encrypted timecode associated with the one frame in a packetized elementary stream (PES), thereby outputting a packetized elementary stream (PES) comprising the plurality of encrypted timecodes.

Claim 2 (original): The method according to claim 1 and wherein the implemented encryption method comprises an asymmetric encryption method.

Claim 3 (original): The method according to claim 1 and wherein the implemented encryption method comprises a symmetric encryption method.

Claim 4 (previously presented): The method according to claims 1 and wherein the timecode comprises an offset from a broadcast headend station time.

Claim 5 (previously presented): The method according to claim 1 and wherein the one frame comprises at least one of the following: video; audio; and data.

Claim 6 (currently amended): A timecode generation method comprising:

receiving an encryption key and an implemented encryption method;

for each one of a plurality of frames, receiving a timecode and an associated decoding time stamp (DTS) associated with the one frame, the DTS occurring in advance of a presentation time stamp (PTS) associated with the one frame;

for each one of the plurality of frames, encrypting the timecode associated with the one frame using the encryption key and the implemented encryption method, thereby producing a plurality of encrypted timecodes; and

for each one of the plurality of encrypted timecodes, placing the encrypted timecode in an encryption container, thereby producing a plurality of encryption containers, each containing an encrypted timecode; and

~~at a time associated with the associated DTS associated with the one frame,~~ for each one of the plurality of frames, for a time associated with the associated DTS associated with the one frame, inserting the encryption container containing the encrypted timecode associated with the one frame in a packetized elementary stream (PES), thereby outputting a packetized elementary stream (PES) comprising the plurality of encrypted timecodes, the PES comprising the plurality of encrypted timecodes not being effective until a time associated with the PTS associated with the one frame.

Claim 7 (original): The method according to claim 6 and wherein the implemented encryption method comprises an asymmetric encryption method.

Claim 8 (original): The method according to claim 6 and wherein the implemented encryption method comprises a symmetric encryption method.

Claim 9 (previously presented): The method according to claim 6 and wherein the timecode comprises an offset from a broadcast headend station time.

Claim 10 (previously presented): The method according to claim 6 and wherein the one frame comprises at least one of the following: video; audio; and data.

Claim 11 (currently amended): A timecode generator comprising:

a first input unit operative to receive an encryption key and an implemented encryption method;

a second input unit operative to receive a timecode and an associated presentation time stamp (PTS) for each one of a plurality of frames;

an encryptor operative to encrypt the timecode for each one of the plurality of frames, using the encryption key and the implemented encryption method, thereby producing a plurality of encrypted timecodes; ~~and~~

a processor operative to place timecode of the plurality of encrypted timecodes in an encryption container, thereby producing a plurality of encryption containers, each containing an encrypted timecode; and

a packetized elementary stream (PES) outputter operative to receive a plurality of encryption containers, each containing an encrypted timecode[[s]] and, [[at]] for a time associated with the associated presentation time stamp (PTS) associated with the one frame, inserting the encryption container containing the encrypted timecode associated with the one frame in a packetized elementary stream, to output a PES comprising the plurality of encrypted timecodes.

Claim 12 (original): The timecode generator according to claim 11 and wherein the encryptor is operative to asymmetrically encrypt the timecode.

Claim 13 (original): The timecode generator according to claim 11 and wherein the encryptor is operative to symmetrically encrypt the timecode.

Claim 14 (previously presented): The timecode generator according to claim 11 and wherein the second input unit receives timecode as an offset from a broadcast headend station time.

Claim 15 (previously presented): The timecode generator according to claim 11 and wherein the one frame comprises at least one of the following: video; audio; and data.

Claim 16 (currently amended): A timecode use method comprising:

receiving an application file comprising a decryption key and an implemented decryption method;

receiving a packetized elementary stream (PES) comprising a plurality of presentation time stamps (PTSs) and a plurality of encryption containers, each of the encryption containers of the plurality of encryption containers containing an encrypted timecode[[s]], each ~~of the plurality of~~encrypted timecode[[s]] being associated with [[a]] one presentation time stamp (PTS); and

running the application file, the running comprising:

performing the following when a system time clock (STC) value equals a ~~PTS~~ value of the one PTS associated with at least one of the ~~plurality of~~ encrypted timecodes:

decrypting the encrypted timecode associated with the ~~PTS~~ value of the one PTS using the decryption key and the implemented encryption method, thereby producing a decrypted timecode.

Claim 17 (original): The method according to claim 16 and wherein the decrypting comprises asymmetric decrypting.

Claim 18 (original): The method according to claim 16 and wherein the decrypting comprises symmetric decrypting.

Claim 19 (previously presented): The method according to claim 16 and wherein each of the plurality of timecodes comprises an offset from a broadcast headend station time.

Claim 20 (currently amended): A timecode use method comprising:

receiving an application file comprising a decryption key and an implemented decryption method;

receiving a packetized elementary stream (PES) comprising:

a plurality of presentation time stamps (PTSs);

a plurality of a decoding time stamps (DTSs); and

a plurality of encryption containers, each of the encryption containers of the plurality of encryption containers containing an encrypted timecode[[s]], each ~~of the plurality of~~encrypted timecode[[s]] being associated with [[a]] one decoding time stamp (DTS), at least one of the ~~plurality of~~ encrypted timecodes requiring that a display be updated at one of a plurality of presentation time stamps (PTS); and

running the application file, the running comprising:

performing the following when a system time clock (STC) value equals a ~~DTS~~ value of the one DTS associated with at least one of the ~~plurality of~~ encrypted timecodes:

decrypting the encrypted timecode associated with the ~~DTS~~ value of the one DTS using the decryption key and the implemented encryption method, thereby producing a decrypted timecode; and

updating the display at the one of the plurality of PTSs.

Claim 21 (original): The method according to claim 20 and wherein the decrypting comprises asymmetric decrypting.

Claim 22 (original): The method according to claim 20 and wherein the decrypting comprises symmetric decrypting.

Claim 23 (previously presented): The method according to claim 20 and wherein each of the plurality of timecodes comprises an offset from a broadcast headend station time.

Claim 24 (currently amended): A timecode handler comprising:

a first input unit operative to receive at least one application file comprising a decryption key and an implemented encryption method;

a second input unit operative to receive a packetized elementary stream (PES) comprising a plurality of encryption containers, each of the encryption containers of the plurality of encryption containers containing an encrypted timecode[[s]], each ~~of the plurality of~~encrypted timecode[[s]] being associated with a presentation time stamp (PTS); and

a decryptor receiving each of the plurality of encrypted timecodes and operative to decrypt each of the plurality of encrypted timecodes using the decryption key and the implemented encryption method when a system time clock (STC) value equals a ~~PTS~~ value of the PTS associated with each of the plurality of encrypted timecodes.

Claim 25 (original): The timecode handler according to claim 24 and wherein the decryptor is operative to asymmetrically decrypt each of the plurality of encrypted timecodes.

Claim 26 (original): The timecode handler according to claim 24 and wherein the decryptor is operative to symmetrically decrypt each of the plurality of encrypted timecodes.

Claim 27 (previously presented): The timecode handler according to claim 24 and wherein each of the plurality of encrypted timecodes comprises an offset from a broadcast headend station time.

Claim 28 (currently amended): A method for timeline protection comprising:

receiving, at a timecode generator, an encryption key and an implemented encryption method;

for each one of a plurality of frames, receiving, at the timecode generator, a timecode and an associated presentation time stamp (PTS) associated with the one frame;

for each one of the plurality of frames, encrypting, at the timecode generator, the timecode associated with the one frame using the encryption key and the implemented encryption method, thereby producing a plurality of encrypted timecodes;

for each one of the plurality of encrypted timecodes, placing the encrypted timecode in an encryption container, thereby producing a plurality of encryption containers, each containing an encrypted timecode; and

~~at a time associated with the associated PTS associated with the one frame,~~ for each one of the plurality of frames, for a time associated with the associated PTS associated with the one frame, inserting the encryption container containing the encrypted timecode associated with the one frame in a packetized elementary stream (PES), thereby outputting a packetized elementary stream (PES) comprising the plurality of encrypted timecodes;

receiving, at a timecode handler, an application file comprising a decryption key and an implemented decryption method;

receiving, at the timecode handler, the PES comprising a plurality of presentation time stamps (PTSs) and a plurality of encryption containers, each of the encryption containers of the plurality of encryption containers containing an encrypted timecode[[s]], each ~~of the plurality of~~encrypted timecode[[s]] being associated with [[a]] one presentation time stamp (PTS); and

running the application file, the running comprising:

at the application file, performing the following when a system time clock (STC) value equals a ~~PTS~~ value of the one PTS associated with at least one of the plurality of encrypted timecodes:

decrypting the encrypted timecode associated with the ~~PTS~~ value of the one PTS using the decryption key and the implemented encryption method, thereby producing a decrypted timecode.

Claim 29 (currently amended): A system for timeline protection comprising:

a timecode generator comprising:

a timecode generator first input unit operative to receive an encryption key and an implemented encryption method;

a timecode generator second input unit operative to receive a timecode and an associated presentation time stamp (PTS) for each one of a plurality of frames;

a timecode generator encryptor operative to encrypt the timecode for each one of the plurality of frames, using the encryption key and the implemented encryption method, thereby producing a plurality of encrypted timecodes;

a timecode container packing unit operative to place each of the plurality of encrypted timecodes in a corresponding encryption container;

a timecode generator packetized elementary stream (PES) outputter operative to receive a plurality of encryption containers, each containting an encrypted timecode[[s]], and, ~~at a time associated with the associated PTS associated with the one frame,~~ for each one of the plurality of frames, for a time associated with the associated PTS associated with the one frame, to output a PES comprising ~~the plurality of encrypted timecodes~~ one of the encryption containers containting an encrypted timecode associated with the one of the plurality of frames; and

a timecode handler comprising:

a timecode handler first input unit operative to receive at least one application file comprising a decryption key and an implemented decryption method;

a timecode handler second input unit active to receive the PES comprising a plurality of ~~encrypted timecodes, each of the plurality of encrypted timecodes being associated with a presentation time stamp (PTS)~~ encryption containers, each of the encryption containers of the plurality of encryption containers containing an encrypted timecode, each encrypted timecode being associated with a presentation time stamp (PTS); and

a timecode handler decryptor receiving each of the plurality of encrypted timecodes and operative to decrypt each of the plurality of encrypted timecodes using the decryption key and the implemented encryption method when a system time clock (STC) value equals a ~~PTS~~ value of the PTS associated with each of the plurality of encrypted timecodes.

Claim 30 (currently amended): A timecode generator comprising:

means for receiving an encryption key and an implemented encryption method;

means for receiving a timecode and an associated presentation time stamp (PTS) associated with each one a plurality of frames;

means for encrypting the timecode associated with each one the plurality of frames using the encryption key and the implemented encryption method, thereby producing a plurality of encrypted timecodes; ~~and~~

means for placing the encrypted timecode in an encryption container, thereby producing a plurality of encryption containers, each containing an encrypted timecode; and

means for outputting a packetized elementary stream (PES) comprising the ~~plurality of encrypted timecodes~~ plurality of encryption containers, each containing an encrypted timecode [[at]] for a time associated with the associated PTS associated with each one the plurality of frames.

Claim 31 (currently amended): A timecode generator comprising:

means for receiving an encryption key and an implemented encryption method;

means for receiving a timecode and an associated decoding time stamp (DTS) for each one of a plurality of frames, the timecode and the DTS being associated with the one frame of a plurality of frames, the DTS occurring in advance of a presentation time stamp (PTS) associated with the one frame;

means for encrypting the timecode associated with the one frame using the encryption key and the implemented encryption method, thereby producing a plurality of encrypted timecodes for each one of the plurality of frames; ~~and~~

means for placing the encrypted timecode into an encryption container, thereby producing a plurality of encryption containers, each containing an encrypted timecode; and

means for outputting a packetized elementary stream (PES) comprising the plurality of encryption containers, each containing an encrypted timecode[[s]], the PES comprising the plurality of encrypted timecodes not being effective until a time associated with the PTS associated with the one frame, the outputting occurring at a time associated with the associated DTS associated with the one frame.

Claim 32 (currently amended): A timecode handler comprising:

means for receiving an application file comprising a decryption key and an implemented decryption method;

means for receiving a packetized elementary stream (PES) comprising a plurality of encryption containers, each of the encryption containers of the plurality of encryption containers containing an encrypted timecode[[s]], each ~~of the plurality of~~encrypted timecode[[s]] being associated with a presentation time stamp (PTS); and

means for running the application file, the running comprising:

performing the following when a system time clock (STC) value equals a ~~PTS~~ value of the PTS associated with at least one of the plurality of encrypted timecodes:

decrypting the encrypted timecode associated with the ~~PTS~~ value of the PTS using the decryption key and the implemented encryption method, thereby producing a decrypted timecode.

Claim 33 (currently amended): A timecode handler comprising:

means for receiving an application file comprising a decryption key and an implemented decryption method;

means for receiving a packetized elementary stream (PES) comprising:

a plurality of presentation time stamps (PTSs);

a plurality of a decoding time stamps (DTSs); and

a plurality of encryption containers, each of the encryption containers of the plurality of encryption containers containing an encrypted

timecode[[s]], each ~~of the plurality of~~encrypted timecode[[s]] being associated with [[a]] one decoding time stamp (DTS), at least one of the ~~plurality of~~ encrypted timecodes requiring that a display be updated at one of a plurality of presentation time stamps (PTS); and

means for running the application file, the running comprising:

performing the following when a system time clock (STC) value equals a ~~DTS~~ value of the one DTS associated with at least one of the ~~plurality of~~ encrypted timecodes:

decrypting the encrypted timecode associated with the ~~DTS~~ value of the DTS using the decryption key and the implemented encryption method, thereby producing a decrypted timecode; and

updating the display at the one of the plurality of PTSs.